EE406021214US

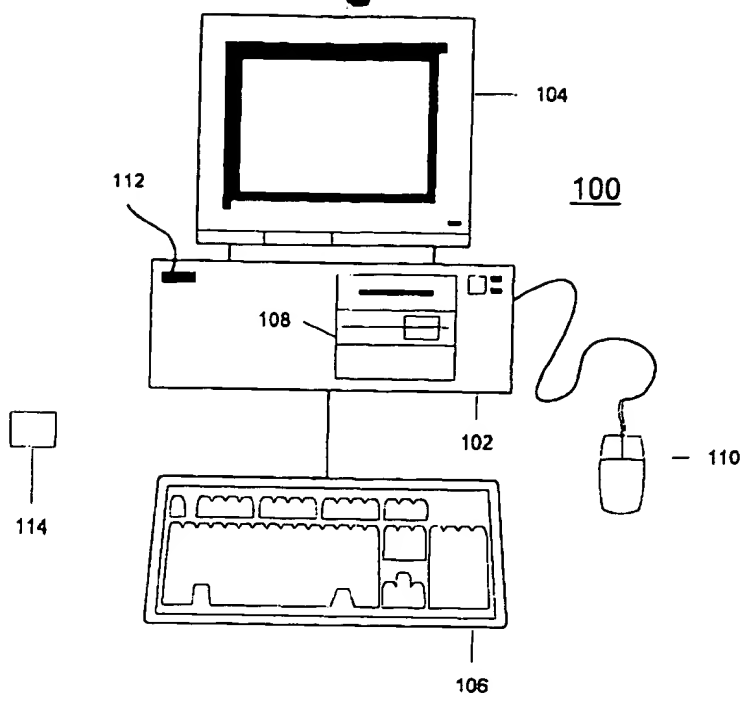

Figure 1
AUS000085US1

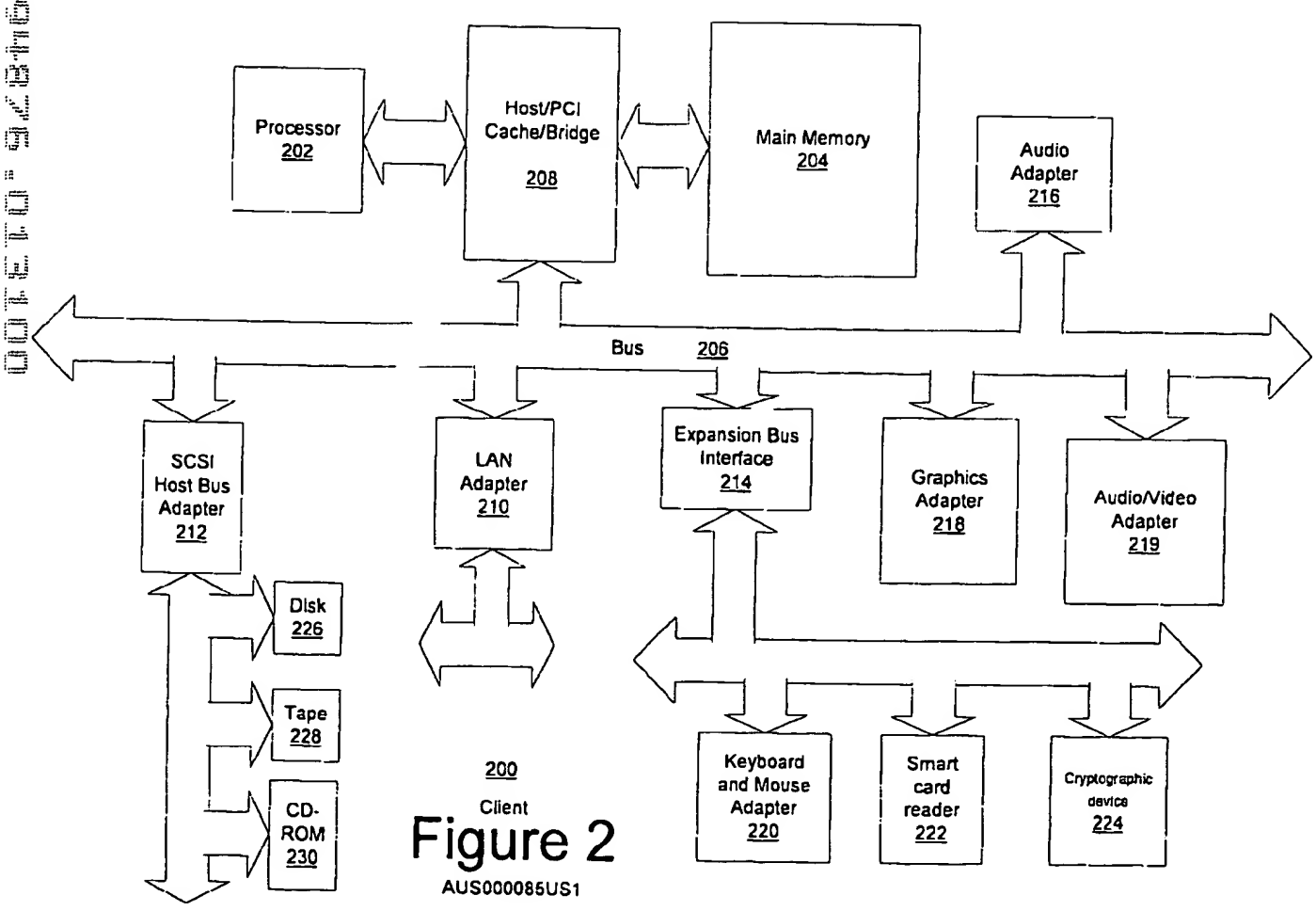

Figure 2
AUS000085US1

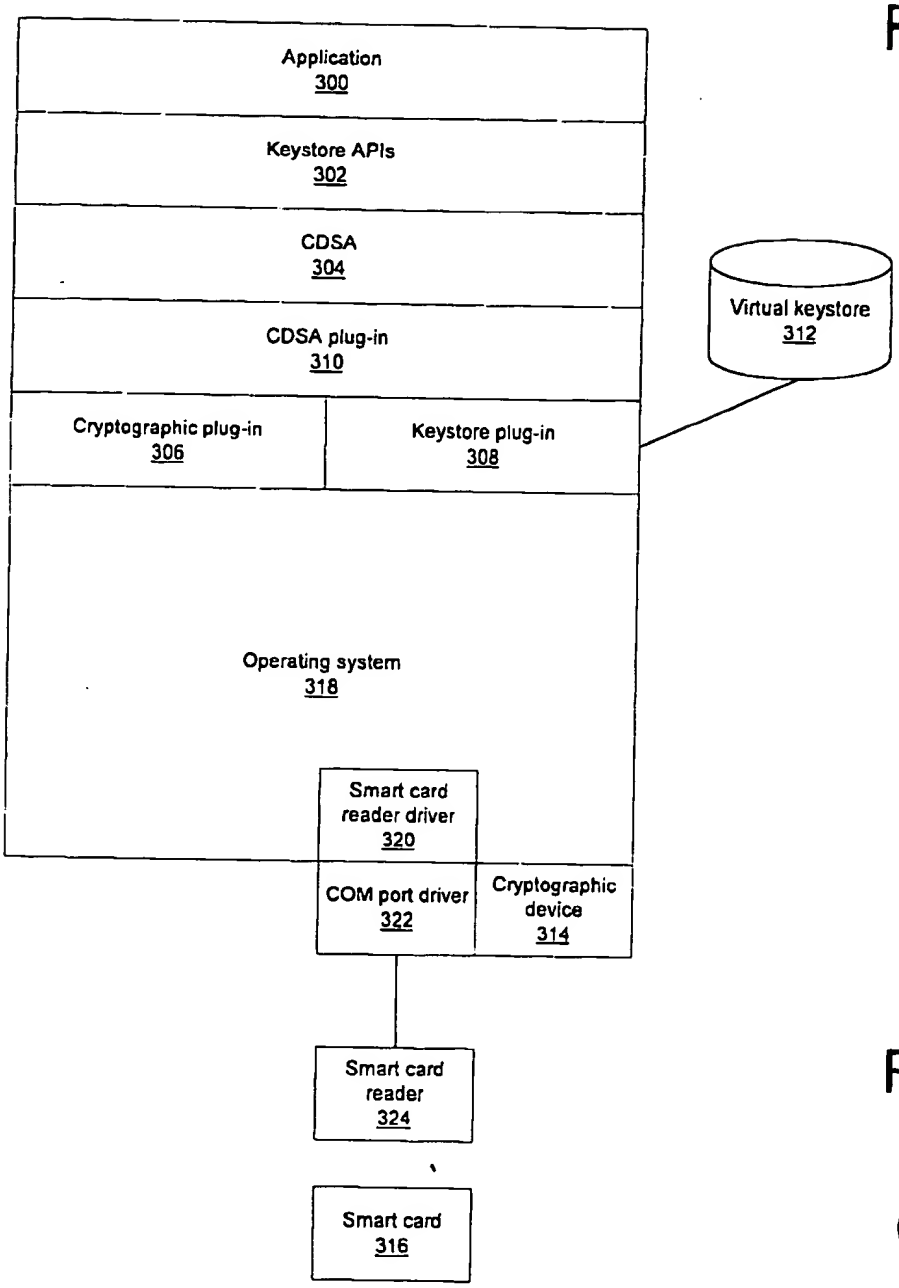

Figure 3
AUS000085US1

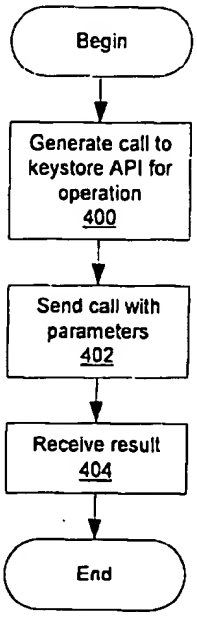

Figure 4
AUS000085US1

Figure 5

AUS000085US1

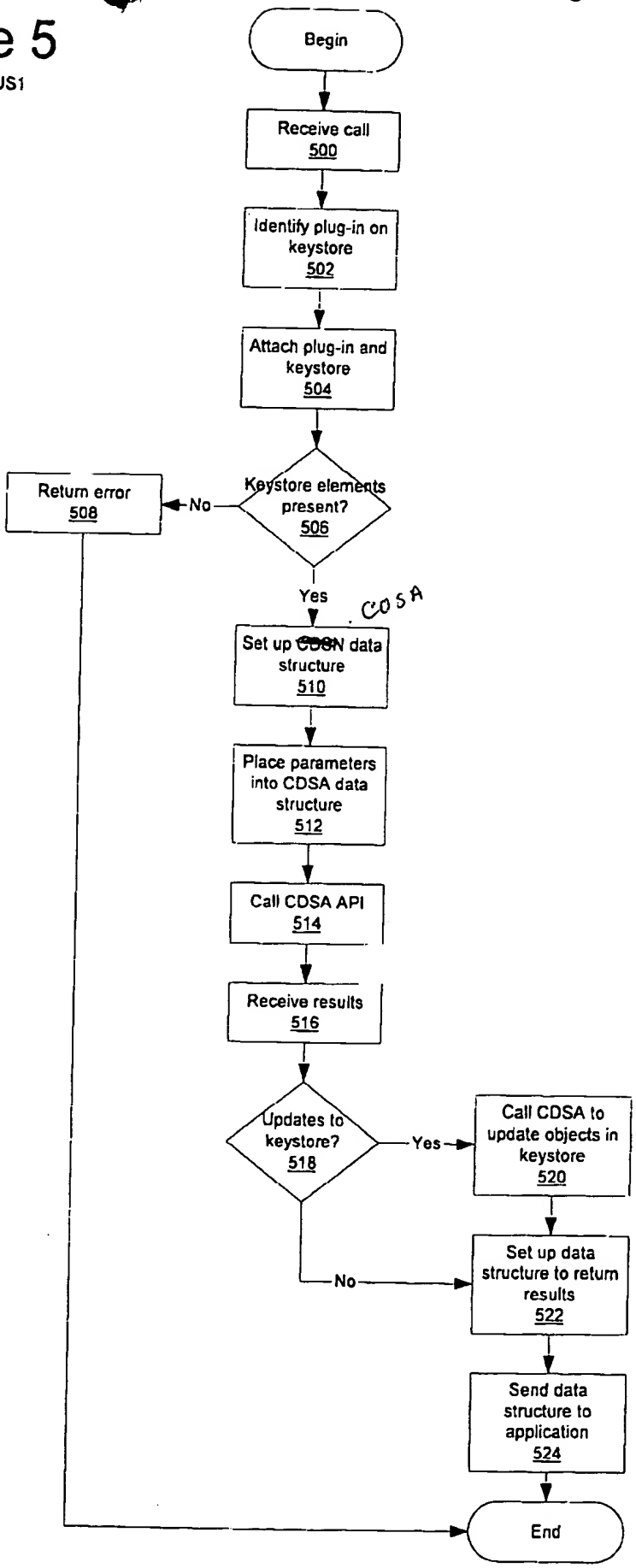

Figure 6

AUS000085US1

600

```
sc_AddCert(

     Get the handle to the keystore database

     Make sure corresponding private key is there

     Get start and end data out of cert to be added
       (dates are attributes stored in the keystore)

     Calculate the subject attribute for the keystore

     Set up CDSA key headers

     Set up key fields into CDSA attributes
          Key label
          Key identifier (index)
          Value of certificate
          Subject of cert
          Class of object
          Type of object (permanent)
          Certificate type
          Privacy of object (can others see it)
          Issuer of cert
          Certificate serial number

     Call CDSA routine to insert the object

     Update the private key's, subject, label & dates to
make sure
          they correspond w/the certificate

     return result of operation
}
```

Docket No. AUS000085US1

Figure 7A

AUS000085US1

sc_ stands for "smart card", as our original implementation was bound to a smart card keystore only

sc_Init - initialize the keystore memory functions
sc_Attach - bind session & login to the keystore
sc_Detach - clean up session to the keystore
sc_GenerateSaveKeypair - generate a public/private key pairs to keystore
sc_CreatePrivateKey - generate and return a private key
sc_StorePrivateKeyByLabel - store an externally generated private key and associate with a provided label
sc_Sign - Create a signature on the input data with the key in the keystore
sc_SignByLabel - Create a signature on the input data referring the signing key by user defined label
sc_Verify - Verify a signature with a certificate in the keystore
sc_RetrievePrivateKeyInfo - Retrieve information about a private key in the keystore
sc_RetrievePrivateKeyInfoByLabel - Retrieve information about a private key in the keystore, referring to the key by a user defined label
sc_RetrieveCertInfo - Retrieve information about a certificate in the keystore
sc_AddCert - Add a certificate into the keystore and associate it with a private key

Figure 7B

AUS000085US1

sc_AddUnattachedCert - Add a certificate into the keystore that is not associated with a private key
sc_StoreGenericByLabel - Store a generic user data
sc_RetrieveGenericByLabel - Retrieve generic user data
sc_DeleteGenericByLabel - Delete generic user data from the keystore
sc_GenericList - Retrieve a list of all generic user data objects from the keystore
sc_IndexList - Retrieve list of all indexs to keystore keys
sc_RetrieveCert - Retrieve a certificate from the keystore
sc_DeleteCert - Delete a certificate from the keystore
sc_HashPublicKey - Function to perform a hash of the public key to use as a key index
sc_CertList - Return a list of certificate indexs in the keystore
sc_DeleteCred - Delete all keys and certificates associated with a key index
sc_DeleteCredByLabel - Delete all keys and certificates associated with a specified label
sc_KeyList - Retrieve a list of all indexs of private keys in the keystore
sc_WrapPrivateKey - Encrypt a private key with another key and return it to the caller
sc_GetKeyPairList - Get list of private keys with associated public keys

Docket No. AUS000085US1